PRESENTATION 3.4.2

N91-17051

RISK ANALYSIS AND MANAGEMENT

RISK ANALYSIS AND MANAGEMENT

H. E. Smith
Lockheed Engineering & Sciences Company

BACKGROUND AND NEED

The complexity and life cycle of both NASA flight and ground systems have undergone a significant increase over the past generation. Additionally, the personnel who possess the design, programmatic and operational knowledge of these systems are becoming unavailable. These changes in turn have dictated the need for a methodology (Figure 1) which provides a common backbone for the forms of risk assessments and analyses which are described in NASA Management Instruction 8070.4, "Risk Management Policy for NASA Manned Flight Programs". The subject NMI provides the following definitions:

1. RISK is exposure to the chance of injury or loss. It It is a function of the possible frequency of the occurrence of an undesired event, of the potential severity of the resulting consequences, and the uncertainties associated with frequency and severity.

2. RISK ASSESSMENT is the process of qualitative risk categorization or quantitative risk estimation, followed by the evaluation of risk significance.

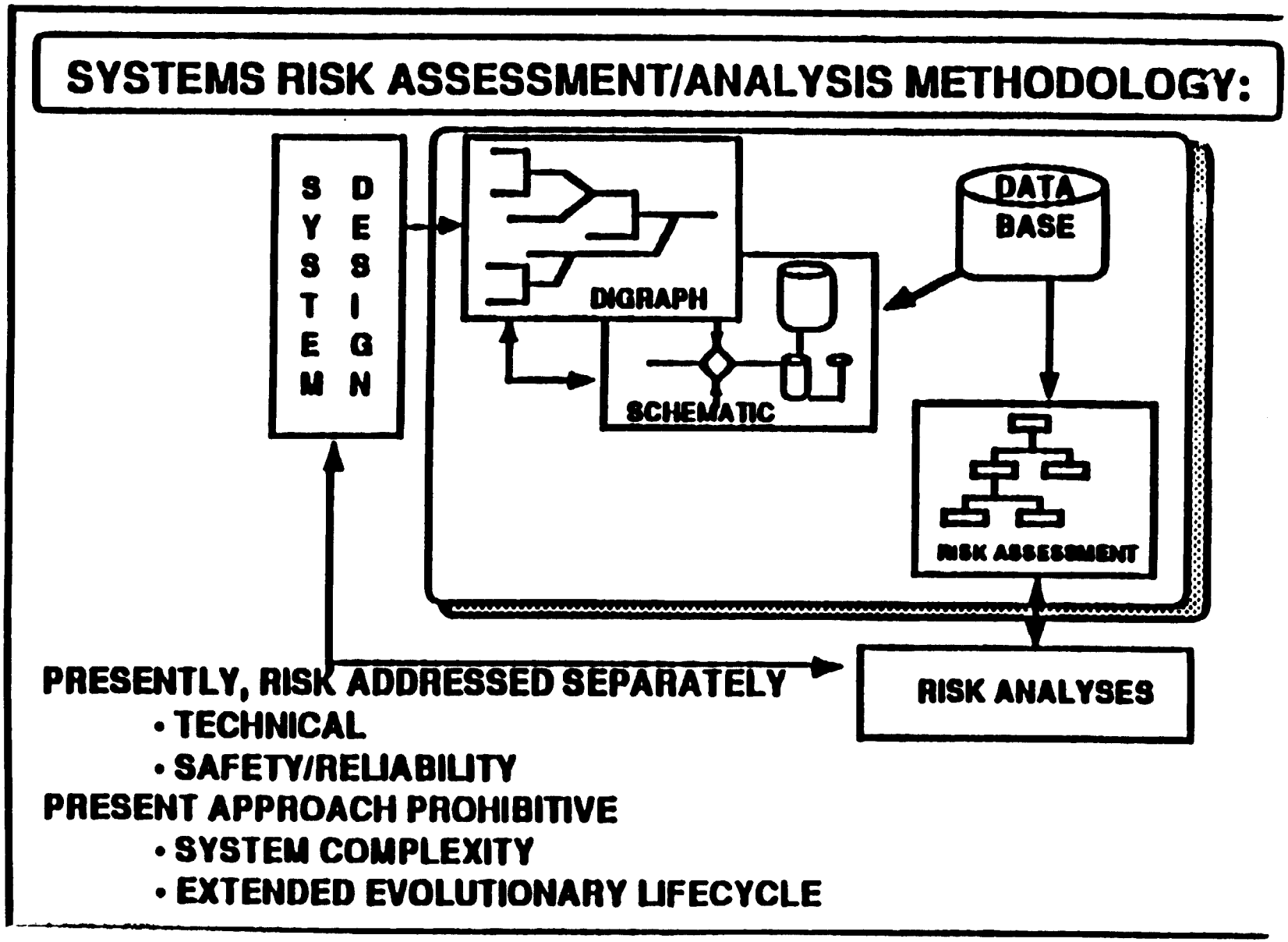
3. RISK MANAGEMENT is the process of balancing risk with cost, schedule, and other programmatic considerations. It consists of risk identification, risk assessment, decision-making on the disposition of risk (acceptance, tolerance through waivers, or mitigation), and tracking the effectiveness of the results of the action resulting from the decision.

Presently, the practiced forms of risk assessment (Failure Modes and Effects Analyses -FMEA's, Fault Tree Analyses-FTA's and Quantitative Risk Assessments -QRA's) are labor-intensive and unique to the system configuration which was investigated. Basically, they do not lend themselves to easy change following a system modification. It appears that a need exists for a methodology (and associated tools) which allows users to:

1) rapidly define and modify system failure paths for both single and multiple failure sources and targets;

2) provide easy reconfiguration of the system design to understand its behavior in failure space in light of design modifications or, in the case of test or flight operations, its tolerance to the next failure; (Note: Behavior in "failure space" is the logical definition of how systems fail as compared to "success space" wherein functional flow diagrams describe how systems operate.)

FIGURE 1


SYSTEMS RISK ASSESSMENT/ANALYSIS METHODOLOGY:
SYSTEM DESIGN
DIGRAPH
SCHEMATIC
DATA BASE
RISK ASSESSMENT
RISK ANALYSES
PRESENTLY, RISK ADDRESSED SEPARATELY
• TECHNICAL
• SAFETY/RELIABILITY
PRESENT APPROACH PROHIBITIVE
• SYSTEM COMPLEXITY
• EXTENDED EVOLUTIONARY LIFECYCLE

3) quantitatively define and assess risk for appropriate component, subsystem and system analyses. The programmatic use of the tools associated with this methodology also provides an approach to the capture and maintenance of the system design knowledge. The tools would readily support design and program decisions, test and flight operations; and personnel training.

TECHNOLOGY STATUS

During the post-Challenger investigation, the National Research Council Shuttle Criticality Review and Hazard Analysis Audit Committee expressed concern that the 1,300 safety-critical failure points were not prioritized based on probability of occurrence. They suggested that an integrated systems assessment be devised which would provide for failure probability quantification.

Pilot Studies

During 1987, several studies (sponsored primarily by various Space Shuttle Program and Project Offices) were undertaken to evaluate the usefulness of QRA methodology, and also identify any areas of concern not previously established.

Reference 1 identifies the most significant lessons learned from these studies. The lessons include the positive value of QRA to:

1) provide quantified risk ranking relative to specified top-level events;

2) capture "corporate knowledge" of the system-under-study far beyond their obvious intent;

3) provide a common forum which encouraged inputs from the various Engineering and SR&QA disciplines;

4) provide a convenient tool for management, in that the resulting risk hierarchy aids in the allocation of normally scarce engineering resources.

On the minus side, the magnitude of the project (assessment of Shuttle systems) taxed the existing software tools to their limit. It was clear that new software support is necessary, and full flight systems studies will require expansions of tool capability.

The final lesson focused on the value of system descriptions for the failure space models. These descriptions were found to be necessary in order to define basic failure events. Analysis personnel found the failure-space model definition to be a labor-intensive paper-and-pencil activity. The value of the model was also diminished with modifications to the system-under-study, and the results were limited to unsharable hardcopy.

Tool Prototyping

The National Space Transportation System Program Office sponsored the Shuttle Critical Function Audit (SCFA) Pathfinder Study during 1988 and 1989. Its objectives are to provide organization of the Shuttle Program knowledge base through system diagrams, descriptions and fault tolerance models; the development of a comprehensive risk assessment database; a QRA capability; and the development of a user interface to the model and data.

Directed graph (digraph) modeling is used to provide the medium for analysis of the failure space models. Modeling experience from this program has indicated the need for providing a user-friendly approach to the simultaneous display of conventional system schematics and failure-space models provided by the digraphs.

Digraph Processor

Presently, the standard for digraph model interpretation is the series of Digraph Matrix Analysis programs which were developed by Analytic Information Processing, Inc. The batch-type programs have been found to be satisfactory in the non-realtime failure-space analysis of large complex systems. However, the programs require significant manual effort in analysis of the digraph model's failure reachability information which result from the mainframe processing. Presently, the vendor is developing a faster PC-based version, which will be available for demonstration, but which still requires manual analysis of the results.

Another prototyping effort, under the leadership of the JSC Avionics Systems Division, is the development of a digraph-based failure analysis algorithm. Their Fault Identification and Risk Management (FIRM) program is currently undergoing beta testing.

User Interface

Lockheed Engineering & Sciences Company has developed the Failure Aanalysis Environment Tool (FEAT) which provides the user with a graphics interface to develop the system digraph models, input them to the digraph processor for analysis; then display the results in color either independently or linked to a subsystem schematic. The prototype tool is undergoing beta testing within the company and elements of the Lyndon B. Johnson Space Center (JSC).

The Mission Operations Directorate of JSC has developed the Shuttle Configuration Analysis Program (SCAP), which provides a ground-based diagnostic capability for indicated Space Shuttle system failure symptoms. The tool demonstrates an application which must be supported by emerging risk assessment technology.

Summary

Present software development accomplishments are indicative of the emerging interest in and increasing efforts to provide risk assessment backbone tools in the manned spacecraft engineering community. Reference 2 indicates that similar efforts are underway in the chemical processes industry and are probably being planned for other complex high-risk ground-based environments. However, it appears that complex flight systems intended for extended manned planetary exploration will drive the technology.

TECHNOLOGY ISSUES AND LESSONS LEARNED

1. The protoyping efforts performed to date have indicated promising concepts toward a flexible and maintainable risk assessment methodology. It appears very important to understand and document the various users' needs which will drive the evolving methodology. The existing prototype tools should be used to confirm the methodology through a series of user-oriented demonstrations. The demonstrations will result in constructive criticism which can lead to customer acceptance of the methodology as it evolves. It is absolutely necessary that the various users in the Design, SR&QA, Test and Operations communities become advocates of the methodology in order to meet the intent of NMI 8070.4.

2. The resulting tools must possess satisfactory portability and flexibility to allow rehosting across computer systems with no significant degradation in usability. The goal is to integrate the tools into major program toolsets.

3. The toolset should provide for easy user training, applications development and operations. Although there will be a need for configuration control in the methodology, it should not preclude the user from being able to transport his application (via floppy disks, if necessary) for discussion with members of the community.

4. A process for establishing and maintaining validity of the models must be included in the methodology.

5. The major using Programs must acknowledge and accept the costs of implementing and maintaining the tools.

REFERENCES

1. SPACE SHUTTLE MAIN PROPULSION PRESSURIZATION SYSTEM PROBABILISTIC RISK ASSESSMENT, FINAL REPORT. JSC-22851, February 1988.

2. IEEE TRANSACTIONS ON RELIABILITY, Vol. 37, No.2; June 1988; "On-Line Hazard Aversion and Fault Diagnosis in Chemical Processes: The Digraph + Fault Tree Method"; Ulerich, N. H. and Powers, G. J.